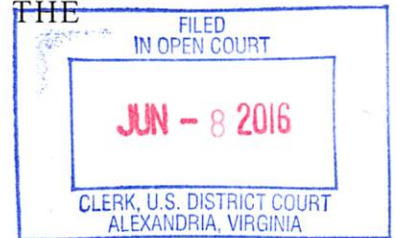


IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

Criminal No. 1:16-CR-140

v.

COUNT ONE: 18 U.S.C. § 371  
Conspiracy to Commit Offenses Against  
the United States

COUNT TWO: 18 U.S.C. § 1030(b)  
Conspiracy to Commit Unauthorized  
Computer Intrusions

PETER ROMAR,  
(a/k/a "PIERRE ROMAR"),  
Defendant.

COUNT THREE: 18 U.S.C. § 1956(h)  
Conspiracy to Launder Monetary  
Instruments

FORFEITURE NOTICE

**INDICTMENT**

June 2016 Term – Alexandria, Virginia

THE GRAND JURY CHARGES THAT:

At all times relevant to this Indictment:

**GENERAL ALLEGATIONS**

1. The Syrian Electronic Army ("SEA") was a group that, beginning in at least fall 2011, was involved in a number of well-publicized computer intrusions in support of the Syrian Government and Syrian president Bashar al-Assad.

2. "Phishing" is the act of attempting to acquire information, such as usernames and passwords, by masquerading as a trustworthy entity in an electronic communication.

"Spearphishing" consists of "phishing" attempts directed at specific individuals or companies.

Individuals engaged in spearphishing may gather personal information about their target to increase the likelihood of succeeding in their spearphishing attempts.

3. Among other methods of computer intrusions that SEA utilized, SEA members would send spearphishing emails to victims that purported to come from a trusted source and that contained hyperlinks to websites that appeared to be trusted websites, but that actually were controlled by the SEA. Any recipient that clicked on such a hyperlink would then be directed to an SEA-controlled website that mimicked a legitimate, trusted website. The recipient would then be asked for credentials, such as a username and password, for access to the supposedly trusted website. For attacks that were successful, at least one recipient provided his or her credentials when prompted. The SEA would then use the stolen credentials to obtain unauthorized access to the computer systems of the target entity. Once the systems were accessed, the SEA would conduct a variety of unauthorized activities, including but not limited to redirecting legitimate Internet traffic, defacing and altering website text, sending messages using the victim's accounts, and conducting further phishing attempts.

4. Co-Conspirator 1, known as "The Shadow," and Co-Conspirator 2, known as "Th3 Pr0," were Syrian nationals located in Syria and members of the SEA.

5. Defendant **PETER ROMAR**, also known as "**PIERRE ROMAR**," ("**ROMAR**"), was a Syrian national residing in Germany.

6. Beginning in or around 2013, ROMAR sought to work with the SEA. For example, on or about April 28, 2013, ROMAR reached out to Co-Conspirator 2 for assistance with computers intrusions that ROMAR represented he was conducting. Co-Conspirator 2 recommended that ROMAR speak with Co-Conspirator 1, and subsequently connected the two of them through social media.

7. Beginning in or around July 2013, ROMAR, Co-Conspirator 1, and others known and unknown to the Grand Jury, extorted or attempted to extort at least 14 different victims in the United States and abroad, after successfully gaining unauthorized access to the victims' computer networks. In total, members of the Conspiracy demanded more than \$500,000 from those 14 victims, although they accepted smaller amounts in many circumstances.

8. Victim 1 was a Europe-based web hosting company.

9. Victim 2 was a California-based dedicated server and web hosting company.

10. Victim 3 was an online media company with offices in the United States. Victim 3 used and controlled a server located in Ashburn, Virginia, within the Eastern District of Virginia.

11. Victim 4 was an online entertainment service with offices in the United States and elsewhere.

12. Victim 5 was a Switzerland-based web hosting company.

13. On or about May 9, 2016, pursuant to Title 18, United State Code, Section 3238, ROMAR was first brought to the Eastern District of Virginia.

**COUNT ONE**

***Conspiring to Commit Offenses Against the United States (18 U.S.C. § 371)***

THE GRAND JURY FURTHER CHARGES THAT:

14. Paragraphs 1 through 13 of the Indictment are incorporated herein by reference.

15. Beginning as early as in or about January 2013, the exact date being unknown to the Grand Jury, and continuing through in or about September 2014, in the Eastern District of Virginia and elsewhere, the defendant, **PETER ROMAR (a/k/a "PIERRE ROMAR")**, did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury, to commit offenses against the United States, that is (i) to transmit in interstate and foreign commerce, with intent to extort from a person, firm, association, and corporation, money and other things of value, a communication containing a threat to injure the property and reputation of the addressee and of another, including Victims 1-5, in violation of Title 18, United States Code, Section 875(d); and (ii) to receive, possess, conceal, and dispose of any money and other property that was obtained from the commission of any offense under this chapter that is punishable by imprisonment for more than one year, including Title 18, United States Code, Section 875(d), knowing the same to have been unlawfully obtained, in violation of Title 18, United States Code, Section 880.

***Manner and Means of the Conspiracy***

16. The manner and means by which the defendant, **PETER ROMAR (a/k/a "PIERRE ROMAR")**, and his co-conspirators sought to accomplish the objects of the conspiracy included, among others, the following:

A. A member of the Conspiracy, in many instances Co-Conspirator 1, obtained unauthorized access to a victim company's computer systems, including by sending spearphishing emails to employees of that company.

B. Once the victim's computer systems were accessed, a member of the Conspiracy would redirect legitimate Internet traffic to or from the victim's systems, deface and alter website text, send messages using the victim's accounts, attempt further phishing attempts, exfiltrate data, or engage in other unauthorized activities.

C. A member of the Conspiracy, in many instances Co-Conspirator 1, would then send emails to employees of the victim companies that indicated his responsibility for the unauthorized access and provided proof of such access. A member of the Conspiracy, in many instances Co-Conspirator 1, would then demand payments from the victim and make threats about what would happen if payment was not received, including but not limited to threats that he would cause further damage to the victim's systems or sell information stolen from the victim.

D. ROMAR, who resided in Germany, would receive payments that Co-Conspirator 1 demanded from victims that could not be transmitted directly to the members of the Conspiracy located in Syria.

#### ***Overt Acts***

17. In furtherance of the conspiracy, and to accomplish its purpose and objects, at least one of the conspirators committed and caused to be committed, in the Eastern District of Virginia and elsewhere, at least one of the following overt acts, among others:

#### **Extortion of Web Hosting Companies in Europe and California (Victims 1 and 2)**

A. On or about October 29, 2013, Co-Conspirator 1 sent an email to Victim 1 and stated that he had "hacked [Victim 1's] websites servers and databases" and "downloaded [sic] it

all.” Co-Conspirator 1 demanded €300,000 in exchange for refraining from selling Victim 1’s databases to other companies.

B. On or about October 30, 2013, Co-Conspirator 1 emailed Victim 1 and lowered his price to €15,200. Victim 1 responded that it could not make bank transfers to Syria because of “sanctions.”

C. On or about October 31, 2013, Co-Conspirator 1 asked Victim 1 to send the money through an intermediary bank, and sent a photograph of his banking information to Victim 1, which listed his true name as the beneficiary of an account and a correspondent bank located in Frankfurt, Germany.

D. On or about November 27, 2013, Co-Conspirator 1 sent an email to Victim 2 stating that he had “hacked your websites servers and databases and i downloaded it all” and requesting money to avoid future unlawful intrusions. Co-Conspirator 1 then threatened that “if you d[o]n’t respond . . . i will hack your website/s . . . i will use your database and your servers [for] my work[.] you have just 1h to respond[.]”

E. When Victim 2 failed to respond to his initial threat, on or about November 27, 2013, Co-Conspirator 1 compromised the company’s domain registration account and modified the routing information for the company’s and some of its clients’ websites. As a result of this compromise, Internet traffic to such sites was redirected to a Conspiracy-controlled website bearing the following message:

HACKED

I told you motherfucker don’t fuck with me go now and cry like a little bitch you and your fucking CEO all your data downloaded [sic] and one of it has been sold.

F. On or about November 28, 2013, when a representative of Victim 2 asked Co-Conspirator 1 by email what the company could do to convince Co-Conspirator 1 to relinquish

control over the re-directed domains, Co-Conspirator 1 demanded €105,000. Co-Conspirator 1 also threatened to sell information regarding vulnerabilities in Victim 2's systems to other hackers if the company failed to comply with his demands.

G. On or about November 28, 2013, Co-Conspirator 1 directed Victim 2 to send the money through an intermediary bank, and sent a photograph of his banking information to Victim 2, which listed his true name as the beneficiary of an account and a correspondent bank located in Frankfurt, Germany.

H. On or about December 6, 2013, the representative of Victim 2 informed Co-Conspirator 1 by email that Victim 2's bank was "giving [Victim 2] a hard time" sending money to Syria, but that Victim 2 was investigating other forms of electronic payment systems to provide funds to Co-Conspirator 1, including PayPal, Bitcoin, and Webmoney. Co-Conspirator 1 replied that none of those payment systems were available to him in Syria, but that he would try to find another method.

I. On or about December 15, 2013, Co-Conspirator 1 reached out to ROMAR through social media to ask for assistance with receiving money in Syria from Victim 1 and Victim 2. Co-Conspirator 1 informed ROMAR that the money was located in two places: the European location of Victim 1 and the United States. Co-Conspirator 1 further stated that he was supposed to receive two payments, and then stated he was receiving money from Victim 1 because he hacked them and worked for them. Co-Conspirator 1 also indicated that if he did not receive payment from Victim 1 that he would declare "war" on them.

J. On or about December 15, 2013, as part of the above communications through social media, ROMAR agreed to assist Co-Conspirator 1 with transferring both payments to

Syria. ROMAR also confirmed that a particular German bank could not transfer money to Syria because of sanctions.

**Extortion Payment Received from Victim 1**

K. On or about December 15, 2013, Co-Conspirator 1 instructed Victim 1 by email to "please send the money to Peter Romar[ ]in Germany via western union."

L. On or about December 20, 2013, after receiving no reply from Victim 1, Co-Conspirator 1 responded with threats in an email entitled "important I hacked your servers":

I will take your not responding is a breach of the Convention  
So I have the right to do what I want with the information . . .

As you know, we ( Ethical Hackers ) have a reputation and we must maintain it  
, I did not took [sic] much time to hack your servers  
But I assure you I will provide plenty of time to I [sic] recover my right

Note:

You have one day to respond

If you do not respond

..... ?? :)

M. On or about December 27, 2013, after Victim 1 again indicated a willingness to pay, Co-Conspirator 1 responded that his "friend" would sign a "contract" that Victim 1 had requested Co-Conspirator 1 sign in order to make the payment through the company's bank account.

N. On December 30, 2013, ROMAR sent an email in English to Victim 1 and attached a signed contract and a scanned image of his German passport.

O. On or about January 2, 2014, Co-Conspirator 1 forwarded ROMAR an email with no new text, but which included in the email chain the text of the email quoted above in paragraph L, entitled "important I hacked your servers."



P. On or about March 6, 2014, Co-Conspirator 1 agreed to reduce the extortion payment from Victim 1 to €5,000 because of difficulties Victim 1 was having in trying to send the money.

Q. On or about March 6, 2014, Co-Conspirator 1 emailed Victim 1 a photograph of ROMAR's bank card and ROMAR's bank account information.

R. On or about March 24, 2014, Co-Conspirator 1 forwarded to ROMAR a nondisclosure agreement that Victim 1 asked that ROMAR sign before sending any money. In his email to ROMAR, Co-Conspirator 1 asked ROMAR to read the agreement and that if ROMAR did not agree with something, to let Co-Conspirator 1 know.

S. On or about March 26, 2014, ROMAR emailed Co-Conspirator 1, addressed him as "The Shadow," and attached a scan of the non-disclosure agreement bearing ROMAR's signature and address in Germany.

T. On or about April 22, 2014, Victim 1 emailed Co-Conspirator 1 and informed him that it had received confirmation that €5,000 was sent to the "German bank account."

**Extortion Payment Received from Victim 2**

U. On or about December 15, 2013, Co-Conspirator 1 sent an email to a representative of Victim 2 and instructed him to send the money to "Peter Romar in Germany via western union."

V. On or about December 25, 2013, Co-Conspirator 1 forwarded his email correspondence with Victim 2 regarding the Western Union payment to ROMAR. In that correspondence, Co-Conspirator 1 had demanded immediate payment from the representative of Victim 2. As part of that email, Co-Conspirator 1 instructed ROMAR, in English, to transmit €1450 to Co-Conspirator 2.

W. On or about December 27, 2013, ROMAR received a Western Union payment from Victim 2 of approximately €1039.13, before fees and taxes.

X. On or about December 27, 2013, ROMAR communicated with Co-Conspirator 1 through social media and stated that he transferred the money from Victim 2 after fees and taxes, approximately €935, to a contact of his in Lebanon. ROMAR informed Co-Conspirator 1 that he needed to first send the money to Lebanon because Western Union would not send the money to Syria. ROMAR further stated that his contact in Lebanon would get the money to Syria.

**Extortion of U.S.-based Online Media Company (Victim 3)**

Y. On or about March 7, 2014, a member of the Conspiracy gained unauthorized access, via a spearphishing attack, to Victim 3's computer servers and databases, including a server located in Ashburn, Virginia, within the Eastern District of Virginia.

Z. On or about March 8, 2014, an employee at Victim 3 received messages from a compromised Google account belonging to Victim 3, in which the communicant, Co-Conspirator 1, took responsibility for the hack. In those communications, Co-Conspirator 1 demanded €20,000 in exchange for stopping "the hack" against the company, refraining from selling the company's database or erasing information from the company's computer systems, and returning information he had taken from the company.

AA. On or about March 10, 2014, after an executive of Victim 3 informed Co-Conspirator 1 that the company could not send funds from a U.S.-based bank to Syria, Co-Conspirator 1 asked the company if it could send the money to "a person in Germany."

BB. On or about March 10, 2014, when an executive of Victim 3 rejected Co-Conspirator 1's proposal, Co-Conspirator 1 threatened to "hack and destroy" the company.

CC. On or about March 19, 2014, after not receiving the demanded payment from Victim 3, Co-Conspirator 1 used Victim 3's customer email lists to distribute spam emails to thousands of Victim 3's customers. Those emails advertised the sale of Victim 3's "hacked" databases for €5000.

**Extortion of Online Entertainment Service with Offices in the United States (Victim 4)**

DD. On or about May 21, 2014, a member of the Conspiracy sent spearphishing emails to employees at Victim 4 that appeared to be from its Chief Executive Officer with a purported hyperlink to a news article regarding Victim 4, but which instead directed recipients to a Conspiracy-controlled website that mimicked the log-in portal for Victim 4's email system. At least one recipient clicked on the embedded hyperlink and, when prompted by the fake log-in portal, entered valid credentials.

EE. On or about May 21, 2014, Co-Conspirator 1 sent the following message to several Victim 4 employees:

...

i hacked all your server and maybe i hacked your databases too  
i can help you to avoid this hack again but i want fees in return

...

so are you interested in this deal or not ?  
DON'T IGNORE THIS EMAIL  
you must to respond at least with YES or NO  
I repeat  
(((( DON'T IGNORE THIS EMAIL ))))

FF. On or about May 23, 2014, Co-Conspirator 1 emailed a representative at Victim 4 a request for €7,500 in exchange for information on how he perpetrated the unlawful intrusion. In that email, Co-Conspirator 1 stated that "... i'm from syria and you should have to send

money outside the U.S. Because U.S. does not deal with the Syrian banks because of USA sanctions[.]”

GG. On or about May 26, 2014, Co-Conspirator 1 indicated to Victim 4 that if there was a problem transferring money to Syria, then Victim 4 could send the money to ROMAR in Germany. Co-Conspirator 1 attached a photograph of ROMAR’s bank card and ROMAR’s bank account information.

HH. On or about May 28, 2014, after Victim 4 indicated it would not pay Co-Conspirator 1, Co-Conspirator 1 sent a threatening email to a representative of Victim 4, which stated, “What do you expect me to do now? :) [D]o you know what I have info [sic] about your company?”

**Extortion of Web Hosting Provider (Victim 5)**

II. On or about July 26, 2014, Co-Conspirator 1 sent an email to several Victim 5 employees containing what appeared to be an employee’s username and password as proof that he “hacked” the company’s database and indicated that “I can help you to avoid this hack again but I want fees in return.”

JJ. On or about July 27, 2014, after a representative of Victim 5 agreed to pay €5,000, Co-Conspirator 1 instructed the representative to send the money to ROMAR and described ROMAR as “my partner and he [is] responsible for receiving money . . . .”

KK. On or about July 27, 2014, Co-Conspirator 1 forwarded a document to ROMAR, which was a scan of a statement indicating that Victim 5 was sending money to ROMAR’s PayPal account in exchange for “ethical penetration testing received.”

LL. On or about July 28, 2014, ROMAR received three payments totaling €5,000 from Victim 5.

MM. Beginning on or about July 31, 2014, ROMAR transferred the payments from Victim 5 (minus nominal fees) from his PayPal account to his bank account in Germany.

All in violation of Title 18, United States Code, Section 371.

**COUNT TWO**

***Conspiring to Commit Unauthorized Computer Intrusions (18 U.S.C. § 1030(b))***

THE GRAND JURY FURTHER CHARGES THAT:

18. Paragraphs 1 through 13 of the Indictment are incorporated herein by reference.

19. Beginning as early as in or about January 2013, the exact date being unknown to the Grand Jury, and continuing through in or about September 2014, in the Eastern District of Virginia and elsewhere, the defendant, **PETER ROMAR (a/k/a "PIERRE ROMAR")**, did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury, to commit the following offenses:

A. to intentionally access a computer without authorization and exceed authorized access, thereby obtaining information from a protected computer, and (i) the offense was committed for purposes of commercial advantage and private financial gain; (ii) the offense was committed in furtherance of a criminal act in violation of the Constitution and the laws of the United States, namely Title 18, United States Code, Sections 875, 880; and (iii) the value of the information obtained exceeded \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2), (c)(2)(B)(i), (c)(2)(B)(ii), (c)(2)(B)(iii);

B. to knowingly, and with intent to defraud, access a protected computer without authorization and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A);

C. to knowingly cause the transmission of a program, information, code, and command, and as result of such conduct intentionally cause damage without authorization to a protected computer, and the offense caused or would have caused (i) loss to persons during a

one-year period from the defendant's course of conduct affecting protected computers aggregating at least \$5,000 in value, and (ii) damage affecting 10 or more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B); and

D. to transmit in interstate and foreign commerce any communication containing any (i) threat to cause damage to a protected computer, (ii) threat to obtain information from a protected computer without authorization and in excess of authorization and to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and (iii) demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, all with the intent to extort from any person any money and other thing of value, in violation of Title 18, United States Code, Sections 1030(a)(7) and (c)(3)(A).

All in violation of Title 18, United States Code, Section 1030(b).

**COUNT THREE**

***Conspiring to Launder Monetary Instruments (18 U.S.C. § 1956(h))***

THE GRAND JURY FURTHER CHARGES THAT:

20. Paragraphs 1 through 13 of the Indictment are incorporated herein by reference.

21. Beginning as early as in or about January 2013, the exact date being unknown to the Grand Jury, and continuing through in or about September 2014, in the Eastern District of Virginia and elsewhere, the defendant, **PETER ROMAR (a/k/a "PIERRE ROMAR")**, did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury, to commit the following offenses against the United States in violation of Title 18, United States Code, Section 1956, to wit:

A. to knowingly conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of a specified unlawful activity, that is an offense under Title 18, United States Code, Section 875 and an offense under Title 18, United States Code, Section 1030, with the intent to promote the carrying on of specified unlawful activity, that is an offense under Title 18, United States Code, Section 1030, and that while conducting and attempting to conduct such financial transaction knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i); and

B. to knowingly conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of specified unlawful activity, that is an offense under Title 18, United States Code, Section 875 and an offense under Title 18, United States Code, Section 1030, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds



of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

C. to transport, transmit and transfer and attempt to transport, transmit and transfer a monetary instrument and funds from a place in the United States to and through a place outside the United States with the intent to promote the carrying on of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(2)(A).

***Manner and Means of the Conspiracy***

22. The manner and means by which the defendant, **PETER ROMAR** (a/k/a **“PIERRE ROMAR”**), and his co-conspirators sought to accomplish the objectives of the conspiracy included, among others, the following:

A. Paragraph 16 of this Indictment is incorporated herein by reference.

B. On or about December 27, 2013, ROMAR received a Western Union payment from Victim 2 of approximately €1039.13, before fees and taxes.

C. On or about July 28, 2014, ROMAR received three payments from Victim 5 totaling €5,000.

All in violation of Title 18, United States Code, Section 1956(h).

**FORFEITURE NOTICE**

THE GRAND JURY HEREBY FINDS THAT:

23. Pursuant to Federal Rule of Criminal Procedure 32.2(a), the United States of America gives notice to defendant **PETER ROMAR (a/k/a "PIERRE ROMAR")** that in the event of his conviction of any of the offenses charged in Counts 1 through 3 of this Indictment, the United States intends to forfeit the defendant's property as further described in this FORFEITURE NOTICE.

24. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, if the defendant, **PETER ROMAR (a/k/a "PIERRE ROMAR")**, is convicted of conspiracy to transmit an interstate communication of threats, in violation of Title 18, United States Code, Section 371, then he shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to the conspiracies.

25. Pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1) and Title 28, United States Code, Section 2461, if the defendant, **PETER ROMAR (a/k/a "PIERRE ROMAR")**, is convicted of conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h), then he shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of Section 1956, or any property traceable to such property, and pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in such an offense, or any property traceable to such property.

26. Pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), if the defendant, **PETER ROMAR (a/k/a "PIERRE ROMAR")**, is convicted of conspiracy to commit unauthorized computer intrusions, in violation of Title 18, United States Code, Section 1030(b), then he shall forfeit to the United States of America his interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation, and any property, real or personal, constituting or derived from any proceeds that he obtained, directly or indirectly, as a result of such violation.

### SUBSTITUTE ASSETS

27. If any of the property described above, as a result of any act or omission of the defendant, **PETER ROMAR (a/k/a "PIERRE ROMAR")**, (a) cannot be located upon the exercise of due diligence; (b) has been transferred or sold to, or deposited with, a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property which cannot be divided without difficulty, the United States of America shall be entitled to and intends to seek forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

Pursuant to Title 18, United States Code, Sections 981, 982, and 1030; Title 21, United States Code, Section 853; Title 28, United States Code, Section 2461.

A TRUE BILL

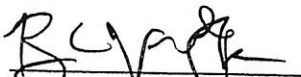
Pursuant to the E-Government Act,  
The original of this page has been filed  
under seal in the Clerk's Office

FOREPERSON

DANA J. BOENTE  
UNITED STATES ATTORNEY

JOHN P. CARLIN  
ASSISTANT ATTORNEY GENERAL  
NATIONAL SECURITY DIVISION

By:

  
Brandon L. Van Grack

Special Assistant United States Attorney

Jay V. Prabhu  
Maya D. Song  
Assistant United States Attorneys

Scott K. McCulloch  
Nathan M.F. Charles  
Trial Attorneys  
Counterintelligence and Export Control Section